ABSTRACT OF THE DISCLOSURE

Methods and apparatuses are provided for limiting access, by users of a networked computer system, to networked services on the computer system. More specifically, the present invention facilitates limiting access by other users to a first user's credential that can be used to facilitate access to networked services. A method includes authenticating a user, determining a credential for that user, and generating a corresponding random secret. The credential is stored in memory that can only be accessed through execution of a local security authority (LSA). The random secret is written to a secret file that is readable and writeable only by the user. When the user initiates an application, a security library associated with the application reads the random secret from the secret file and passes the secret to the LSA. The LSA identifies the credential corresponding to that secret and return a credential handle to the application client via the security library. The application client can use the credential handle to have the LSA use the credential on its behalf; in the Kerberos case, the LSA obtains GSSAPI Kerberos tokens and returns them to the application. The technique is also used in combination with the Unix setuid mechanism to allow one or more programs to have all of the user's network rights while all other programs have one of one or more subsets of the user's rights. Additional embodiments of the present invention also include computer readable medium with program instructions and a computer system configured to perform the above operations.